DTI – ĂNIMA EDUCAÇÃO

Política de Segurança de Informações e uso de recursos computacionais

Normas e procedimentos de utilização de recursos tecnológicos

Administrativo

2010

POLÍTICAS DO DEPARTAMENTO DE TECNOLOGIA		
ănima EDUCAÇÃO	**Segurança de Informações e Utilização de Recursos Computacionais**	**Elaborado em:** **28/04/2010** **Revisado em:** **26/07/2010** **Aprovado em:** **16/08/2010**

Elaborado por:

DTI:

- Edson Eduardo S. Santos (DTI ĂNIMA)
- Tiago Campos Carrusca (DTI ĂNIMA)

Revisado por:

- Heleno Carlos Fernandes (jurídico ĂNIMA)
- Maria Elisabeth Ferraz (Diretoria Acadêmica ĂNIMA)

Aprovado por:

- Bruno Henrique de Macedo Machado (DTI ĂNIMA)
- Cristiane Lima Gatti Guimarães (Gestão de Pessoas UNA)
- Elisete Helena Goncalves (Gestão de Pessoas UNIMONTE)
- Flavio Korn (Diretor de Serviços ĂNIMA)
- Lícia Boechat Assbú Janones (Gestão de Pessoas ĂNIMA)
- Luis Alberto Rocha Benfica (Jurídico ĂNIMA)
- Manoella Vasconcellos Costa (Gestão de Pessoas UNIBH)

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ĂNIMA EDUCAÇÃO

Garantir a **informação** como bem essencial da companhia, respeitando sua confidencialidade, assegurando sua continuidade e a usando de maneira ética.

I. INTRODUÇÃO

As informações, resumidamente são dados que, tratados adequadamente modificam quantitativamente e qualitativamente os ativos de uma organização. Essas informações portanto agregam valores, e por sua vez, devem ser protegidas, tendo em vista a quantidade de ameaças a que estão sujeitas (NBR ISO/IEC 17799:2000, pág. VI).

> A informação pode existir de diversas formas, ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meio eletrônico, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou meio através do qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida adequadamente. (NBR ISO/IEC 17799, setembro 2001).

Desde o surgimento da internet e consequentemente a unificação da rede mundial, as organizações e seus sistemas de informações e redes se deparam frequentemente com constantes e crescentes ameaças como: invasão, hackers, vírus, spam, espionagem, vandalismo, etc.

A Segurança de Informações protege as informações por meio de normas, políticas, práticas, procedimentos, conscientização, treinamentos, estruturas e softwares, agindo diretamente sobre essas ameaças. (NBR ISO/IEC 17799:2000, pág. VI).

Este documento foi elaborado fundamentado nos principais agentes da Segurança de Informações, citados acima.

1. ESTRUTURA DO DTI (DEPARTAMENTO DE TECNOLOGIA E INFORMAÇÃO)

- ✓ **Gerência de Tecnologia da Informação:** o Gerente de TI é responsável pela gestão de sua equipe e contato com os clientes, tendo como foco principal alcançar os objetivos propostos, gerenciando projetos, orçamentos, custos, contratos externos, SLA's externos, processos de TI, políticas, comunicação e marketing de TI.

- ✓ **Coordenação de Sistemas de Informação:** O Coordenador de sistemas é responsável por projetar, planejar, desenvolver, testar, manter e suportar sistemas de informação como: ERP, sistemas acadêmicos, aplicações complementares, sistemas próprios e BI (Business Intelligence), sendo de extrema importância que todos os projetos e objetivos concluídos sejam informados ao Gerente de TI.

- ✓ **Coordenação de Infraestrutura de TI e Telecomunicações:** O Coordenador de Infraestrutura de TI e Telecomunicações é responsável pela gerência da estrutura da rede corporativa e telecomunicações. Deve planejar, desenvolver, acompanhar e manter projetos e soluções com relação à infraestrutura de rede e Telecom. Todos os projetos e objetivos concluídos devem ser informados ao Gerente de TI.

- ✓ **Coordenação de Atendimento ao cliente interno (NSI):** O Coordenador do NSI é responsável por organizar e gerir todos os projetos relacionados ao suporte de informática, atendimento aos clientes internos, externos, salas de aula e laboratórios, tornando-se responsável pelos equipamentos de informática e audiovisuais situados nesses locais, devendo organizar a estrutura e o fluxo, desde o atendimento do *Service Desk*, até a entrega dos serviços. Todos os projetos e objetivos concluídos devem ser informados ao Gerente de TI.

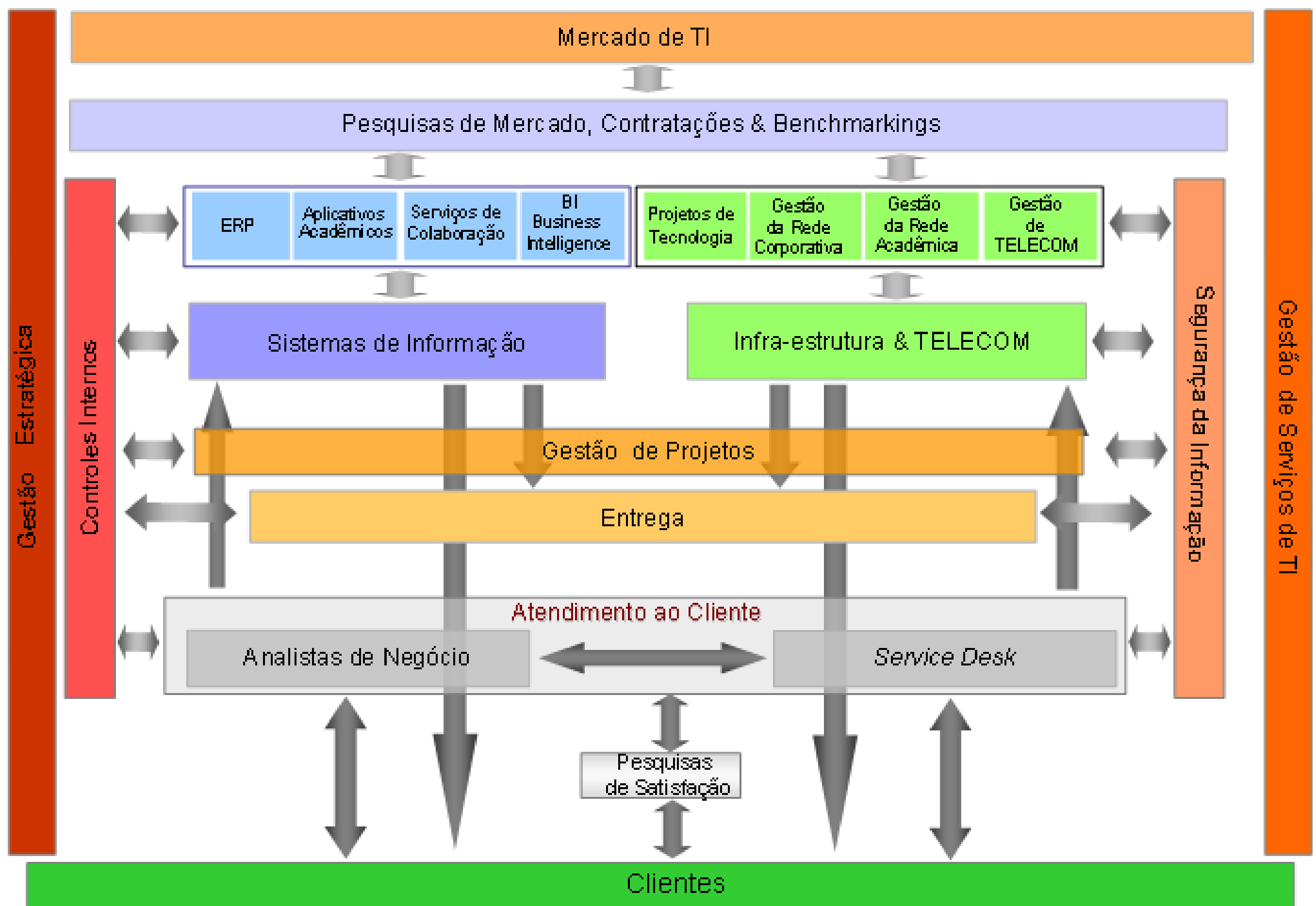
2. SERVIÇOS DTI

O Departamento de Tecnologia tem por finalidade prover soluções de tecnologia da informação, automação dos processos de trabalho, comunicação eletrônica e armazenamento e segurança de dados para os usuários das empresas que compõem o grupo ĂNIMA

EDUCAÇÃO, bem como prover e manter todos os recursos computacionais das Instituições, zelando pela integridade, segurança e bom desempenho dos equipamentos e sistemas por ele mantidos.

3. DIVISÃO DE RESPONSABILIDADES:

- ✓ Planejamento e gerenciamento (Gerência);
- ✓ Tecnologia e Infraestrutura (Redes);
- ✓ Segurança da informação (Analista de Segurança);



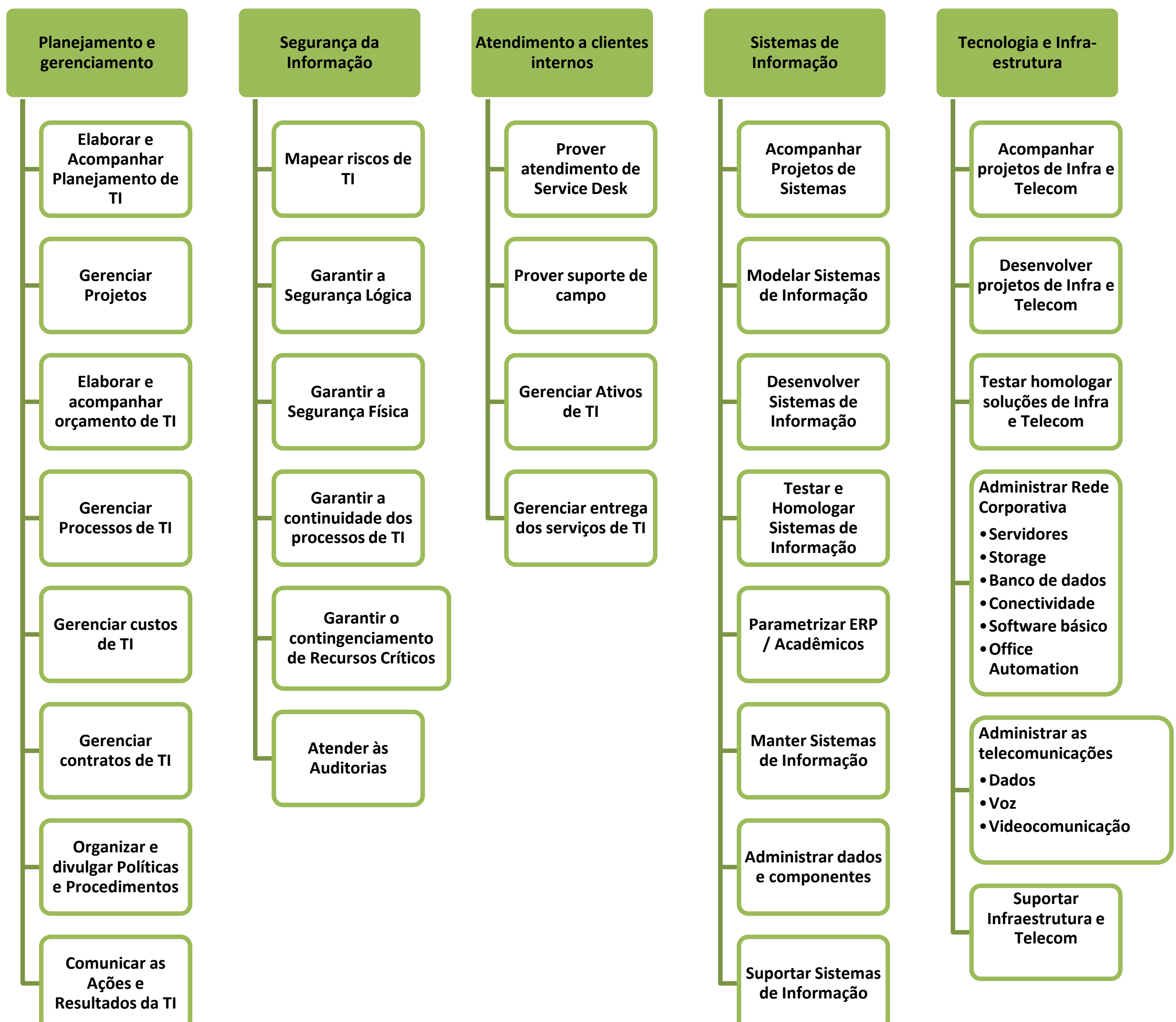
- ✓ Sistemas de Informação (Desenvolvimento de Sistemas);

4. ATENDIMENTO A CLIENTES INTERNOS:

Fluxo de atendimento do DTI:

Com o objetivo de fornecer uma melhor visualização das responsabilidades e serviços do Departamento de Tecnologia da Informação, foi elaborado um portfólio de serviços mapeados de acordo com cada setor.

Visão geral do portfólio de serviços de tecnologia:



II. OBJETIVOS DESTA POLÍTICA

O objetivo desta política é orientar os colaboradores, estagiários, prestadores de serviços e visitantes, sobre as diretrizes referentes à Segurança de Informações e Uso de Recursos Computacionais implantadas nas empresas que compõem o Grupo ĂNIMA, buscando proteger ativos da informação de sua propriedade, ou sob sua custódia, contra ameaças internas ou externas, deliberadas ou acidentais.

III. APLICAÇÃO

Esta política aplica-se a todos os usuários dos sistemas e dos recursos computacionais das empresas que compõem o Grupo ĂNIMA, e das Instituições de Ensino a elas vinculadas, sendo estes os funcionários, estagiários, alunos, colaboradores, terceiros ou visitantes.

IV. PRINCÍPIOS

A segurança da informação é baseada na preservação dos seguintes princípios:

- ✓ **Confidencialidade**: garantia de que o acesso à informação é restrito a pessoas autorizadas, ou seja, proteção à informação privada contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação;

- ✓ **Integridade**: A integridade consiste em evitar que dados sejam apagados, ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de integridade está relacionado à segurança que os dados não foram modificados por pessoas não autorizadas;

- ✓ **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos necessários sempre que for preciso. Para isso, é de extrema importância que os serviços prestados pelo sistema sejam protegidos de forma que não sejam degradados, ou se tornem indisponíveis sem autorização;

- ✓ **Autenticidade**: está associada à identificação de um usuário ou computador. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos**;**

V. RESPONSABILIDADES

Dos colaboradores, estagiários e prestadores de serviços que utilizam recursos de informática:

1. Conhecer e agir conforme o conteúdo contido nesta política e nas documentações normativas relacionadas às suas atividades;
2. Conhecer e assinar o termo de responsabilidade, por meio do qual se comprometerão formalmente a seguir a política de segurança, tomando ciência das punições impostas em caso de seu não cumprimento;

Do Gestor da Segurança da Informação:

1. Facilitar a implantação desta política através da elaboração e divulgação de políticas, normas e procedimentos apropriados;

2. Promover a constituição do Comitê de Segurança, que será constituído por um representante de cada área a seguir:

   - Gerência de TI;
   - Coordenação de Sistemas de TI;
   - Coordenação de Infraestrutura de TI;
   - Gestão de Pessoas;
   - Departamento de Pessoal;
   - Diretoria Jurídica;
   - Diretoria Acadêmica.

3. Analisar criticamente as causas de incidentes de segurança da informação e suportar planos de ação para a melhoria da Gestão da Segurança da Informação, com o Departamento de Tecnologia da Informação;

4. Alocar os recursos necessários para iniciativas que visem aumentar o nível de segurança da informação na organização;

5. Difundir a cultura de segurança da informação nas empresas que compõem o Grupo ĂNIMA, com o apoio do Comitê de Segurança;

6. Criar e gerar relatórios de disponibilidade de hosts e serviços;

7. Criar e gerar relatórios de utilização de internet;

8. Propor programas de treinamento em segurança da informação aos funcionários e prestadores de serviço, quando necessário;

O Comitê de Segurança deverá:

1. Garantir a correta e consistente execução dos controles estabelecidos;

2. Apoiar o Gestor de Segurança da Informação;

3. Apoiar iniciativas de melhoria da TI;

4. Gerenciar a atualização da Política de Segurança, por meio de reuniões periódicas para definição e atualização de processos da mesma;

5. Providenciar, junto à Comunicação Interna, um Plano de Divulgação da Política de Segurança;

6. Dirimir questões de incidentes de segurança não previstos e que não tenham suporte nas normas vigentes;

O Departamento de Tecnologia deverá:

1. Prover a infraestrutura e os recursos de tecnologia da informação necessários ao cumprimento desta política;

2. Analisar criticamente as causas de incidentes de segurança da informação e suportar planos de ação para a melhoria da Gestão da Segurança da Informação com o responsável pela mesma;

3. Analisar, por meio de relatórios técnicos, todos os dados estatísticos sobre ataques ou qualquer outra ameaça à infraestrutura de tecnologia da informação das empresas que compõem o Grupo ĂNIMA;

4. Instalar software de acesso remoto nas estações de trabalho com o intuito de aperfeiçoar os processos de monitoramento e atendimento dos usuários;

5. Remover softwares instalados que não condizem com as atividades institucionais;

6. Executar programas de inventário, a fim de identificar softwares sem licenciamento ou danosos à rede;

7. Realocar recursos computacionais visando o aperfeiçoamento dos procedimentos administrativos da Instituição;

8. Analisar e averiguar a rede corporativa, a fim de detectar fluxo indevido de informações, intrusos e ataques aos sistemas e serviços de rede;

9. Aplicar filtros na rede corporativa, de qualquer natureza, para minimizar riscos aos ativos de informação da Instituição;

10. Instalar ferramentas de gerenciamento de rede, a fim de manter o controle e disponibilidade das atividades institucionais;

11. Executar aplicativos na estação de trabalho para sincronizar dados com servidores, bem como configurar aplicativos automaticamente;

12. Criar regras de bloqueio de sites que possuam conteúdos indevidos a fim de gerenciar o uso da ferramenta;

13. Personalizar o acesso à internet, solicitando login e senha aos usuários, a fim de gerenciar o uso da ferramenta;

14. Usar ferramentas para evitar que cheguem mensagens indesejadas aos usuários, com a implantação de AntiSpam;

15. Excluir automaticamente mensagens dos servidores com conteúdos indevidos ou que possuam códigos maliciosos;

16. Limitar o uso da banda de internet e caixa postal dos usuários, de acordo com as políticas da Instituição;

17. Interromper os serviços de internet e correio eletrônico corporativo quando necessário;

18. Solicitar, quando necessário, a troca de senhas de rede, de sistemas, de Internet e de Correio Eletrônico Corporativo e exigir senhas complexas;

19. Excluir as contas de rede, de sistemas, de Internet e de Correio Eletrônico Corporativo dos usuários desligados da Instituição;

O Gestão de Pessoas e o Departamento de Pessoal deverão:

1. Apoiar, mediante ações de treinamento e conscientização, as ações e programas de promoção do cumprimento e de mitigação de violações a esta política;
2. Repassar as informações sobre funcionários desligados imediatamente após assinatura do termo de rescisão de contrato, para controle e bloqueio de acessos;
3. No ato da contratação, colher a assinatura no Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários.

O Departamento Jurídico deverá:

1. Validar e atualizar o Termo de Responsabilidade de utilização de recursos computacionais;
2. Avaliar, quando solicitado, as normas e os Procedimentos de Segurança da Informação elaborados pelo DTI.
3. Representar e defender judicialmente a Instituição, se necessário, em caso de transgressão das normas, por parte de alunos, professores, colaboradores e etc.

VI. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO E UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS

Quanto à solicitação de equipamentos, softwares e serviços de informática:

1. Toda solicitação de equipamentos, softwares ou serviços deverá ser feita ao Departamento de Tecnologia e Informação (DTI) por meio do sistema de chamados (Help Desk);

2. Em caso de impossibilidade de acesso ao sistema de chamados (Help Desk) ou dúvidas na abertura do chamado, entrar em contato com o suporte técnico, de segunda à sexta-feira, de 8 às 22h, através dos telefones:

   Belo Horizonte, (31) 3319-9336;

   Santos, (13) 3228-2126;

3. Deverá ser aberto um chamado para cada solicitação a ser atendida;

4. Todo chamado submetido ao DTI será analisado de modo a considerar primeiramente as possibilidades de manutenção corretiva ou realocação de recursos e, em último caso, compra ou contratação;

5. O DTI tem autonomia para alocar recursos de informática em toda a Instituição, bem como sugerir soluções e emitir pareceres técnicos, de acordo com o solicitado;

6. Definem-se como equipamentos de informática quaisquer artigos do tipo hardware utilizados na Instituição e gerenciados pelo DTI, tais como computadores (servidores e desktops), notebooks, pockets, palmtops, discos rígidos, memórias, cabos específicos, mouses, teclados, webcams, kits multimídia, gravadoras de CD-ROM e/ou DVD, leitoras de CD-ROM e/ou DVD, monitores, impressoras, scanners, ativos de rede, etc.;

7. Classificação/Aplicações de Estações de Trabalho:

   a. Estações desktop Tipo I – Orientadas a usuários de aplicações de automação de escritório, ERP, aplicações de baixo consumo de recursos de hardware;

   b. Estações desktop Tipo II - Orientadas a usuários de uso médio de recursos computacionais, como simuladores matemáticos, processadores gráficos, etc.;

   c. Estações desktop Tipo III - Orientadas a usuários de uso intensivo de recursos computacionais, como, sistemas de CAD, edição de imagens e vídeo, etc.;

8. Definem-se como softwares, todo e qualquer programa instalado nos computadores da Instituição, seja por tempo determinado ou não, independentemente de sua finalidade e/ou setor no qual estará sendo utilizado;

9. Definem-se como serviços relacionados, todo e qualquer serviço relacionado a cabeamento estruturado (ponto de rede), manutenção, consultoria ou assessoria nos equipamentos ou softwares da Instituição;

Quanto ao uso das estações de trabalho:

1. Os usuários são responsáveis diretos pela utilização dos recursos computacionais a eles confiados, em concordância com as diretrizes deste regulamento. São considerados recursos computacionais: conjunto formado por um gabinete CPU, monitor, teclado, mouse e sistema operacional; notebooks; impressoras; Palmtops; smartphones; softwares; internet; intranet; correio eletrônico corporativo e sistemas em geral;

2. O usuário deverá sempre bloquear a estação de trabalho quando se ausentar, uma vez que ele é o responsável por tudo que venha a ser executado a partir desta.

10. Qualquer ocorrência (quebra, falha, mau funcionamento, incidente, desaparecimento) relacionada aos equipamentos de informática deverá ser informada imediatamente à Área de Tecnologia, pelo sistema de chamados (Help Desk), ou através dos telefones:

    Belo Horizonte, (31) 3319-9336;

    Santos, (13) 3228-2126;

3. É **vedado** ao usuário:
    a. Abrir o gabinete da estação de trabalho e instalar dispositivos de hardware, por quaisquer motivos;
    b. Instalar qualquer sistema operacional ou softwares, inclusive livres ou gratuitos, na estação de trabalho, sem autorização prévia do DTI;
    c. Fazer cópia, para uso externo, de softwares adquiridos ou desenvolvidos pela ĂNIMA;
    d. Realizar conexões de rede, bem como conexões de recursos computacionais pessoais na rede administrativa;
    e. Compartilhar a unidade do disco rígido (raiz) entre usuários;

f. Danificar ou remover as placas de identificação ou de patrimônio dos equipamentos;
g. Realizar a transmissão ou posse de informações que impliquem violação de direitos autorais (pirataria) ou de propriedade da informação;
h. Utilizar servidores da ĂNIMA para armazenamento de informações ou arquivos pessoais;

Quanto ao uso das impressoras e copiadoras:

1. O serviço de impressão de grande porte (setores que imprimem mais de 3.000 páginas por mês) é prestado por empresa terceirizada. O DTI recebe relatórios mensais de todas as impressões feitas nesses equipamentos, bem como pode gerar relatórios a qualquer momento, a fim de auditoria.

2. Cabe ao DTI definir que tipo de impressora cada setor deve utilizar;

3. As solicitações de reparo no equipamento e troca de periféricos devem ser realizadas por meio do sistema de chamados do Grupo ĂNIMA;

4. O controle de papel deve ser feito por cada setor que utiliza o equipamento terceirizado, e as solicitações devem ser feitas para o almoxarifado, por meio de pedidos no Datasul.

Quanto à utilização de serviços gráficos da empresa terceirizada:

1. Os serviços gráficos (cópias simples, impressões de provas, cópias coloridas, etc.), serão prestados por empresa terceirizada, que manterá, sempre que possível, locais de atendimento em cada uma das unidades das Instituições do Grupo ĂNIMA.

2. Todos os serviços prestados pela empresa terceirizada poderão ser solicitados via protocolo de requisições que se encontram no NSI ou nas coordenações de curso (exclusivo para impressões acadêmicas, como provas, exercícios avaliativos entre outros);

3. Os custos do serviço serão debitados no centro de custo do setor solicitante, no fechamento de caixa do mês. Cabe ao líder do setor prever verba para esses serviços (exceto Unimonte);

Quanto ao acesso a rede corporativa e seus serviços:

1. O acesso ao ambiente informatizado deverá ser concedido unicamente por meio de identificação (conta ou login) e de senha associada;

2. A criação do login é padronizada: utiliza-se o primeiro e o último nome do usuário separados por um ponto (.). Em caso de duplicidade de login, o padrão poderá ser modificado e avaliado pelo DTI;

3. A conta do usuário será válida por tempo determinado, enquanto vigorar o contrato de trabalho do funcionário ou do prestador de serviço;

4. Quando for constatada a necessidade de acesso à rede por terceiros, o mesmo poderá ser solicitado pelo responsável do setor, via sistema de chamados. O acesso será concedido apenas se aprovado pelo DTI após análise;

5. É dever do usuário a proteção de suas credenciais de acesso a sistemas de informação. O detentor da conta e senha deverá assumir a responsabilidade pela guarda, descrição ou sigilo das operações decorrentes do seu uso. Recomenda-se a troca de senha mensalmente, feita pelo próprio usuário através da intranet, ou pelo “alterar senha” do Windows;

6. A implantação de perfis de acesso será realizada com base no princípio de privilégio mínimo;

7. A utilização do acesso à Internet nas empresas do Grupo ĂNIMA deve estar prioritariamente relacionada às tarefas desempenhadas pelo funcionário. Uso pessoal de ordem eventual é permitido, desde que não consuma recursos significativos de tempo ou interfira na produtividade pessoal;

8. O cadastro do funcionário no ambiente informatizado deverá ser solicitado à área de tecnologia, imediatamente após sua admissão, pelo líder imediato, por meio do

sistema de chamados. Conforme informado anteriormente, deverá ser aberto um chamado para cada solicitação a ser atendida;

9. É vetado o acesso a sites de conteúdo criminoso, de apostas ou pornografia. A ĂNIMA irá restringir os acessos a sites que considerar alheios aos objetivos do grupo e monitorar consultas de usuários, com o objetivo de garantir segurança e adequação no uso deste recurso;

10. O acesso a serviços como FTP, Telnet e outros devem ser solicitados formalmente pelo responsável da área interessada, à Área de Tecnologia, justificando o pedido;

11. O desligamento de funcionário será informado imediatamente pelo Departamento de Pessoal à área de Tecnologia, que tomará as providências necessárias para o cancelamento da conta do funcionário, bem como para a devolução, se houver, dos equipamentos de informática de propriedade das empresas do Grupo ĂNIMA, por ele utilizados;

12. Caso seja necessário o compartilhamento de arquivos entre usuários, este poderá ser realizado somente na pasta desejada, devendo as configurações de compartilhamento aplicadas, assim como as devidas permissões, serem disponibilizadas apenas ao usuário beneficiário, devendo o usuário que disponibilizou o compartilhamento, removê-lo após o uso;

13. É permitido aos usuários proprietários de notebook o acesso à rede corporativa, desde que sejam autorizados pelo DTI após solicitação via sistema de chamados. A permissão de uso de notebooks e demais computadores portáteis será concedida após o cumprimento de todas as normas de segurança, ou seja, é obrigatório que o Sistema Operacional e o software de antivírus estejam atualizados;

14. É **vedado** ao usuário:
    a. Revelar a terceiros sua identificação de usuário e senha de acesso à rede ou qualquer sistema da Instituição;

b. Alterar qualquer configuração de rede de computadores, devendo solicitar ao DTI, por meio do sistema de chamados, necessidades específicas de conexão à rede ou modificação de configurações;
c. Burlar ou tentar burlar os dispositivos de segurança da rede;
d. Capturar dados na rede corporativa que coloquem em risco a confidencialidade dos documentos, arquivos e o fluxo de dados entre as estações;
e. Acessar ou navegar em sites que não sejam ligados ao desenvolvimento da atividade de trabalho;
f. Fazer download de arquivos executáveis ou de multimídia, mesmo que estejam compactados sem autorização prévia do DTI;
g. Usar a internet para finalidades desnecessárias e prejudiciais aos ativos de informação das empresas do Grupo ĂNIMA e de outras Instituições;
h. A instalação de equipamentos de rede sem fio (Access Point) sem autorização prévia do DTI;

15. Rede Wireless (Administrativa)
    - ✓ A rede wireless do grupo ĂNIMA EDUCAÇÃO é destinada à utilização de internet, portanto o suporte não é fornecido se o funcionário desejar trabalhar pelo notebook por meio da rede wireless;
    - ✓ As configurações de acesso à rede wireless serão realizadas somente pela equipe do NSI especializada e responsável por essa tarefa;
    - ✓ É de responsabilidade da equipe de Redes a configuração de qualquer Access Point localizado em quaisquer campi;
16. Os serviços de Internet, Intranet e Correio Eletrônico Corporativo não podem ser utilizados para atividades ilícitas, contrárias aos interesses legítimos da Instituição, ou fora do contexto das atividades de trabalho, ou em violação às regras fixadas neste documento;
17. VPN (Virtual Private Network)
    a) A utilização da VPN está limitada somente aos funcionários;
    b) O acesso à rede VPN deve ser solicitado por meio do sistema de chamados, pelo líder imediato do funcionário;

c) A configuração do cliente VPN deve ser de responsabilidade do usuário, ou seja, o DTI não se responsabiliza pela configuração do cliente da estação de trabalho remota, o DTI disponibilizará um manual de instruções ao usuário para configuração da estação de trabalho remota;

d) O trabalho a distância está restrito aos funcionários e prestadores de serviço, autorizados diretamente por seus gestores, conforme as regras de acesso definidas pelo DTI;

Quanto ao uso e seleção de senhas:

1. Senhas são de uso pessoal e intransferível, sendo sua manutenção e confidencialidade, responsabilidade de seu proprietário;
2. Senhas não devem ser registradas em papel, ou em qualquer meio sem controle ou caracterizado como de acesso público;
3. Uma senha deve ser criada com no mínimo 8 (oito) caracteres e deve ser atualizada pelo usuário no primeiro logon. Essa atualização se dará no próprio sistema de autenticação;
4. A conta será bloqueada, caso o usuário digite a senha incorretamente cinco vezes consecutivas;
5. Senhas temporárias ou iniciais devem ser alteradas no primeiro acesso ao sistema, conforme regra estabelecida pelos analistas de rede e sistemas aplicativos;
6. Senhas devem ser alteradas pelos usuários sempre que existir qualquer indicação de possível comprometimento do sistema ou das próprias senhas. Recomenda-se a mudança de senha mensalmente;

Quanto ao uso de mensagens eletrônicas (e-mail):

1. O correio eletrônico é um recurso disponibilizado pelas empresas do Grupo ĂNIMA para uso profissional, sendo passível de auditoria;
2. O uso para fins particulares do correio eletrônico disponibilizado pelas empresas do Grupo ĂNIMA, de ordem eventual, é permitido, desde que não consuma recursos significativos de tempo e não interfira na produtividade. Tal uso não isenta o usuário do processo de auditoria;

3. A integridade e o backup de mensagens armazenadas fora dos servidores corporativos serão de responsabilidade do usuário;
4. O usuário poderá solicitar, por meio do sistema de chamados, a realização do backup de suas mensagens;
5. Mensagens de correio eletrônico são consideradas correspondências oficiais. Assim sendo, recomenda-se a identificação do usuário emitente, mediante inserção de informações ao final do texto, com a sua assinatura padrão contendo as seguintes informações:
   - ✓ Nome do remetente completo;
   - ✓ Cargo;
   - ✓ Setor;
   - ✓ Telefone;
   - ✓ E-mail
6. Com relação ao conteúdo das mensagens de correio eletrônico, cabe ao usuário:
   a. Não enviar, sem autorização formal do responsável pela área, quaisquer documentos contendo material confidencial ou de uso interno das empresas do Grupo ĂNIMA;
   b. Não utilizar o correio eletrônico das empresas do Grupo ĂNIMA para veicular correntes, filmes, músicas, pornografia, discriminação de raça, sexo e credo, bem como para veicular mensagens de movimentos políticos ou outros conteúdos não relacionados à finalidade de trabalho;
   c. Não utilizar palavras de baixo calão ou ofensas a qualquer outro usuário, seja interno ou externo;
   d. Jamais executar arquivos anexados com extensões .exe, .com, .bat, .vbs, .scr, sendo que estes devem ser eliminados imediatamente;
7. É expressamente proibida a transmissão de mensagens de correio eletrônico indiscriminadamente para todos os funcionários. As exceções serão definidas pela a área de Comunicação Interna;
8. Recomenda-se não enviar mensagens que contenham arquivos anexos que ultrapassem 5MB. Cabe salientar que o limite para envio de cada mensagem é de 10MB;
9. A área de Tecnologia irá verificar, regularmente, o uso do correio eletrônico, com objetivo de detectar ameaças à segurança ou uso indevido do mesmo. Para tal, poderão

ser utilizados softwares específicos com funcionalidades de bloqueio proativo de spams.

Quanto ao uso de computação móvel:

1. São itens que pertencem à computação móvel: notebooks, netbooks, smartphones, placas de internet 3G e palmtops;

2. Classificação de Notebooks
    a. Notebook Tipo I – Fornecido pelo NSI, para empréstimo, aos professores, para apresentação de slides e utilização de softwares em aula (UNIMONTE e UNI-BH);
    b. Notebook Tipo II – Orientados a funcionários que demandam maior mobilidade e poder de processamento;
    c. Cabe ao Gestão de Pessoas, conjuntamente com o DTI, as avaliações para disponibilização de notebooks;
3. Os usuários da computação móvel (notebooks) devem estar cientes dos seguintes riscos e aceitar as seguintes responsabilidades:
    a. A segurança física e lógica existente no local de trabalho a distância deve ser avaliada, e controles apropriados serão implantados para minimizar o risco de roubos de informações ou ocorrência de incidentes que comprometam a segurança dos sistemas das empresas do Grupo ĂNIMA;
    b. É obrigatória a utilização da corrente de segurança (cabo de aço), devendo a solicitação ser realizada por meio do sistema de chamados (Help Desk);
    c. O acesso a informações ou a recursos, por pessoas não autorizadas, será de responsabilidade do responsável pelo equipamento móvel em questão.
    d. Quaisquer incidentes de segurança que ocorram nas localidades remotas de trabalho, tais como roubos, invasões, infecções por vírus, deverão ser imediatamente comunicadas à área de Tecnologia, para que as medidas apropriadas sejam tomadas.

Quanto à instalação e utilização de softwares:

1. A utilização de softwares será disponibilizada mediante os seguintes procedimentos:
    a. Validação dos requisitos técnicos definidos pela área de tecnologia;

b. Disponibilidade e aquisição de licença de software;
c. Instalação, pela área de Tecnologia, do software adquirido;

2. Os equipamentos de informática funcionarão somente com softwares regularmente adquiridos e licenciados junto a seus fornecedores ou representantes, ou ainda, aqueles desenvolvidos pelo quadro de funcionários da Instituição;
3. A área de Tecnologia, periodicamente, irá efetuar auditoria nas estações de trabalho, objetivando manter o padrão corporativo de softwares nos equipamentos;
4. A instalação de softwares sobre os quais a ĂNIMA não detenha direitos, e que visem atender interesses de patrocinadoras ou Empresas com as quais mantenha acordo operacional, deverá ser precedida de contrato que preserve a ĂNIMA de qualquer ônus;
5. Todos os servidores corporativos e estações de trabalho serão protegidos por software de antivírus homologado, devendo estar sempre ativo e atualizado, seguindo as configurações definidas pela área de Tecnologia, não podendo ser removido pelo usuário em nenhuma hipótese;

Quanto à realização de backup, cópia de segurança e restauração de dados:

1. A área de Tecnologia é responsável por efetuar as operações de backup, cópia de segurança e restauração das informações armazenadas **nos servidores da rede** corporativa da ĂNIMA;
    a. Entende-se por backup as operações de cópia feitas diariamente, com prazo curto de vida, para garantir o retorno de falhas no sistema;
    b. Entende-se por cópias de Segurança as operações de cópia feitas em períodos de tempo mais longo, sendo as mídias retidas, também, por prazos mais longos.
    c. Os backups devem ser feitos regularmente conforme conceitos acima, portanto serão realizados backups, diários, semanais, mensais e anuais.
2. A responsabilidade pela guarda e execução das cópias de segurança das informações armazenadas **nas estações de trabalho** será do usuário da estação de trabalho.
3. Não será realizado, pela área de Tecnologia, backup ou cópia de segurança de nenhuma informação ou arquivo armazenado nessas estações.
4. Quando necessário, o proprietário da Informação deve solicitar formalmente à área de Tecnologia, a restauração da cópia de segurança da informação armazenada nos

servidores, respeitando as periodicidades determinadas na política de cópia de segurança das informações.

5. O usuário poderá solicitar um backup de sua estação de trabalho, mediante formalização pelo sistema de chamados. O prazo para a entrega do backup deve ser acordado no ato da solicitação com o responsável do NSI do campus respectivo;

Quanto à manutenção e administração do ambiente:

1. Alterações em locais que afetem ou demandem novos recursos de infraestrutura de rede, devem ser informados à área de Tecnologia, para as devidas providências.
2. Qualquer mudança no local de instalação do equipamento deve ser solicitada à Área de Tecnologia, para adequação dos inventários físicos dos mesmos.
3. Qualquer mudança do usuário responsável pelo equipamento deverá ser comunicada imediatamente à Área de Tecnologia.
4. Programas em produção devem estar armazenados fisicamente em local diferente dos programas em desenvolvimento e/ou testes, sendo devidamente protegidos contra acesso não autorizado.
5. As empresas do Grupo ĂNIMA, por meio da área de Tecnologia, poderão padronizar a configuração das estações de trabalho, com a utilização de papéis de parede, protetores de tela, menus de navegação, etc.

Quanto ao uso dos sistemas de informação:

1. A concessão e autorização de perfis de autorizações de usuários para acesso aos sistemas de informação deverão ser solicitadas à área de tecnologia, imediatamente após sua admissão, pelo líder imediato, por meio do sistema de chamados (Help Desk). Conforme informado anteriormente, deverá ser aberto um chamado para cada solicitação a ser atendida;
2. Perfis de autorizações são direitos de acesso à funções dos sistemas de informação, de acordo com as tarefas executadas pelos funcionários da ĂNIMA.
3. Cabe à supervisão do usuário definir qual o perfil adequado de autorizações para acessar cada sistema, devendo este perfil estar documentado na solicitação.
4. Cabe também à supervisão do usuário certificar que o nível de acesso concedido está adequado aos propósitos do negócio e que não compromete à segregação de funções.

5. Todas as solicitações de criação e alteração de perfis deverão ser armazenadas para permitir auditorias futuras.
6. Cabe à Área de Tecnologia remover os direitos e as contas de acesso aos sistemas de informação de usuários que tenham sido desligados da ĂNIMA desde que comunicados previamente ou revogar os direitos em caso de transferência concedendo as permissões necessárias para a nova função.

Quanto ao uso dos laboratórios de informática:

1. Do acesso
   a. Os laboratórios de informática são administrados pelo Departamento de Tecnologia e Informação (DTI);
   b. Os laboratório de informática são destinados para ao acadêmico de alunos e professores da Instituição, utilizados, prioritariamente, para aulas práticas;
   c. Os funcionários poderão utilizar as dependências dos laboratórios prioritariamente para execução de treinamentos, ou durante os horários de almoço e descanso, desde que os laboratórios estejam identificados como de acesso livre;
   d. Para obter acesso aos laboratórios de informática, cada aluno, professor ou funcionário deverá possuir login e senha;
   e. São considerados alunos, os estudantes regularmente matriculados na Instituição, e professores, docentes contratados para ministrar aulas ou outras atividades acadêmicas na Instituição;
   f. Poderão ser concedidos acessos especiais, desde que devidamente autorizados pelo DTI;
   g. Os usuários terão acesso aos recursos dos laboratórios de informática de acordo com o seu perfil, curso ou departamento, respeitando as diretrizes estabelecidas pela Instituição;
   h. Todo usuário tem a obrigação de estar ciente das normas e dos regulamentos que regem o funcionamento dos laboratórios de informática da Instituição, disponíveis no seu acesso restrito do site;
   i. Quando o cadastramento não ocorrer de forma automática, o usuário deverá se dirigir ao Núcleo de Suporte à Informática (NSI) do seu campus e requisitar o

login e senha, já para Unimonte, o usuário deverá se dirigir ao Multiatendimento (CAA) para abertura de chamado específico;

j. O acesso aos laboratórios de informática deverá ser feito por meio dos computadores disponíveis, após informação de login e da senha para autenticação do usuário;
k. É permitido a funcionários e alunos o uso de notebooks desde que esteja ciente que a responsabilidade de uso e configuração é do proprietário;

2. Do horário de funcionamento
   a. Os horários de funcionamento dos laboratórios de informática são de segunda a sexta-feira, das 7:20h às 22:35h e aos sábados sob demanda, das coordenações de curso;
   b. Os usuários deverão respeitar os horários de funcionamento dos laboratórios de informática, visto que os equipamentos deverão ser desligados no horário previsto para encerramento;

3. Da estrutura, da impressão e do armazenamento de dados:
   a. Os laboratórios de informática dispõem de computadores com softwares licenciados instalados, rede local, serviço de impressão a laser, acesso à internet e serviço técnico especializado;
   b. Caso necessário, funcionários, alunos, professores, coordenadores, visitantes ou terceiros poderão comprar créditos para impressão pela empresa terceirizada, prestadora de serviços gráficos;
   c. A impressão deve ser retirada pelo aluno, ou professor, ou funcionário, em um dos totens ou nas lojas da copiadora, no prazo de até 6 horas contados após o envio da impressão, mediante a inserção de login e senha no sistema;

Quanto às Videoconferências:

1. Internas
   a. As videoconferências internas são as realizadas entre os funcionários do grupo ĂNIMA, dentro de suas dependências;
   b. Devem ser agendadas pelo e-mail de videoconferência do campus com no mínimo 6 horas de antecedência;

c. Os equipamentos serão testados pelo NSI com no mínimo 30 minutos de antecedência;

2. Externas (de um equipamento do grupo ĂNIMA para outra empresa)
   a. As videoconferências externas são as realizadas entre os funcionários do grupo ĂNIMA dentro de suas dependências com participação de outras empresas;
   b. Devem ser agendadas pelo e-mail de videoconferência do campus, com no mínimo 2 (dois) dias úteis de antecedência;
   c. Os equipamentos serão testados pelo NSI com no mínimo 24 horas de antecedência;
   d. Utilizamos o equipamento do fabricante Polycom, sendo que o protocolo de comunicação utilizado é TCP/IP, portanto não estabelecemos videoconferências com equipamentos não compatíveis com o mesmo e/ou que utilizem ISDN;

3. Os formulários de agendamentos serão impressos e afixados na porta da sala de videoconferência com 24 horas de antecedência, ou até o prazo mínimo estabelecido acima. Caso não exista agendamento para videoconferência, a sala poderá ser utilizada pra outras reuniões, com o devido registro no formulário de agendamento;

4. Existem instruções de uso dos equipamentos em todas as salas. Caso ocorra algum erro durante a utilização do equipamento, o NSI deverá ser prontamente contatado através do telefone existente nessas instruções;

5. Os equipamentos dependem do fornecimento de rede elétrica e de dados, portanto, imprevistos podem ocorrer no fornecimento destes serviços, interrompendo as videoconferências;

Quanto à aquisição de estações de trabalho, notebooks e servidores:

1. Condições técnicas e comerciais para o fornecimento:
   a. O fornecimento se dá de acordo com a disponibilidade orçamentária para a execução de projetos;

b. As solicitações de compra de equipamentos devem ser, preferencialmente, dirigidas ao setor de compras, sendo as informações referentes às especificações de cada equipamento, de responsabilidade do solicitante;

2. Classificação de estações:
    a. Estações desktop Tipo I – Orientadas a usuários de aplicações de automação de escritório, ERP, aplicações de baixo consumo de recursos de hardware;
    b. Estações desktop Tipo II - Orientadas a usuários de uso médio de recursos computacionais, como simuladores matemáticos, processadores gráficos, etc.;
    c. Estações desktop Tipo III - Orientadas a usuários de uso intensivo de recursos computacionais, como, sistemas de CAD, edição de imagens e vídeo, etc.;

3. Classificação de notebooks:
    a. Notebook Tipo I – Fornecido pelo NSI, por empréstimo aos professores, para apresentação de slides e utilização de softwares em aula (UNIMONTE e UNI-BH);
    b. Notebook Tipo II – Orientados a usuários que demandam maior mobilidade e poder de processamento.

4. Classificação de servidores:

    A solicitação de aquisição de servidores está diretamente à demanda de projetos e serviços a serem desenvolvidos e disponibilizados.

VII. DAS PENALIDADES

1. Ao usuário que descumprir o estabelecido nesta Política de Segurança de Informações, serão aplicadas medidas disciplinares de acordo com a gravidade do fato, com segue:
   a. Gravidade baixa: advertência formal feita pelo gerente responsável;
   b. Gravidade média: suspensão por até 03 (três) dias, aplicada pelo gerente responsável;
   c. Gravidade alta: demissão feita pelo empregador;

2. O Anexo I desta Política de Segurança de Informações e Utilização de Recursos Computacionais disporá sobre faltas, gravidade da infração e medida aplicável;

3. Os casos não constantes do Anexo I serão decididos pelo Comitê de Segurança, que deverá sugerir a penalidade a ser aplicada, elaborando parecer e enviando ao gerente responsável, para análise e aplicação da medida disciplinar;

4. As penalidades sofridas pelos usuários serão registradas em sua ficha funcional.

VIII. DISPOSIÇÕES GERAIS

1. Todos os usuários deverão assinar o termo de responsabilidade de uso dos recursos computacionais, declarando pleno conhecimento dos termos desse regulamento;
2. O termo de responsabilidade de uso dos recursos computacionais preenchido e assinado deverá ser encaminhado ao departamento de pessoal para ser arquivado no prontuário do funcionário;
3. Todas as regras estabelecidas neste regulamento se aplicam também aos prestadores de serviço;
4. É de inteira responsabilidade do usuário, o uso de qualquer recurso computacional que não seja patrimônio da Instituição. Portanto, qualquer desgaste ou dano de equipamentos, decorrentes do seu uso nas dependências da Instituição, será da sua inteira responsabilidade.

Anexo I

Quadro exemplificativo de infrações às regras de utilização de recursos computacionais

Incidente	Gravidade	Medida disciplinar
Uso indevido da Marca da Empresa na Internet e associação a conteúdo não apropriado	Média	Advertência formal pelo gerente responsável
Uso indevido de internet e estação de trabalho para finalidade particular (não houve incidente de segurança – vírus)	Baixa	Advertência formal pelo gerente responsável
Uso indevido de e-mail corporativo para passar boatos e piadas (não houve vazamento de informação confidencial)	Média	Advertência formal pelo gerente responsável
Empréstimo de senha de login para colega de trabalho e terceirizado (senha de gestor com segregação de funções)	Média	Advertência formal pelo gerente responsável
Pasta com software de jogo pirata instalado (crime e quebra de política)	Alta	Desligamento em função da gravidade
Pastas de diretório com vídeos e arquivos pornográficos	Alta	Desligamento em função da gravidade
Envio de e-mail para pessoa errada com vazamento de informação confidencial e restrita (fato relevante)	Média	Advertência formal pelo gerente responsável

Quadro de penalidades em caso de furto, perda, ou mau uso - administrativo

Incidente	Gravidade	Medida Disciplinar
Perda ou extravio de notebook (*)	Alta	Desconto, em folha, do bem depreciado
Furto de notebook dentro da instituição, sem utilização de equipamento de segurança fornecido pelo DTI (*)	Alta	Desconto, em folha, do bem depreciado
Furto de notebook dentro da instituição, com utilização de equipamento de segurança fornecido pelo DTI (*)	-	Avaliação de arrombamento pela Infraestrutura
Furto de notebook fora da instituição (*)	Alta	Desconto, em folha, do bem depreciado

Quadro de penalidades em caso de Furto, perda, ou mau uso – docente

Incidente	Gravidade	Medida disciplinar
Perda ou extravio de notebook fornecido ao professor, para utilização em aulas	Alta	Desconto, em folha, do bem depreciado
Perda ou extravio de Datashow fornecido, ao professor para utilização em aulas	Alta	Desconto, em folha, do bem depreciado

***Prazo de reposição de equipamento definido entre DTI e líder de área, de acordo com a disponibilidade de verba.**
*** Casos específicos e/ou excepcionais serão devidamente analisados pelo Comitê de Segurança, Líder imediato e Gestão de Pessoas.**

IX. REFERÊNCIAS

1. NBR ISO/IEC 17799:2000.